UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,297	07/22/2003	James W. O'Toole JR.	CIS03-08(6535)	7810

47654 7590 10/26/2006

DAVID E. HUANG, ESQ.
BAINWOOD HUANG & ASSOCIATES LLC
2 CONNECTOR ROAD
SUITE 2A
WESTBOROUGH, MA 01581

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/624,297	**Applicant(s)** O'TOOLE ET AL.	
	Examiner Devin Almeida	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 July 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *10/08/2004*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 7/22/2003. Claims 1-38 were received for consideration. No preliminary amendments for the claims were filed. Currently claims 1-38 are under consideration.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 11/08/2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 4-5 and 7-11 rejected under 35 U.S.C. 102(e) as being anticipated by Park (U.S. Patent Application Publication # 2004/0085445). With respect to claim 1, Park teaches a method for obtaining video data, the method comprising: providing a control signal to a video data acquisition system (see Park paragraph 0016-0019 and

0023); receiving an output signal from the data acquisition system in response to providing the control signal, the output signal including video data captured by the video data acquisition system (see Park paragraph 0016-0019); and verifying an authenticity of the video data from the data acquisition system by checking that the received output signal includes modifications according to the control signal (see Park paragraph 0016-0019).

With respect to claim 2, providing a control signal includes: providing a control signal that includes a key for encrypting the video data transmitted by the video data acquisition system (see Park paragraphs 0018-0019 and 0023).

With respect to claim 4, providing a control signal includes: providing a control signal that includes a command to overlay a recognizable pattern onto the video data such that the recognizable pattern appears on a viewing display when the video data is replayed (see Park paragraph 0069-0073).

With respect to claim 5, overlaying a recognizable pattern onto the video data includes: modifying a value of a text string associated with the video data that appears on the display when the video data is replayed at a later time (see Park paragraph 0069-0073).

With respect to claim 7, An apparatus for authenticating video data including a processor that provides a control signal to a video data acquisition system, the processor receiving an output signal from the data acquisition system including video data in response to providing the control signal, the processor verifying an authenticity of the video data from the data acquisition system by checking that the received output signal includes modifications according to the control signal (see Park paragraph 0016-0019 and 0023).

With respect to claim 8, the control signal includes a key for encrypting the video data transmitted by the video data acquisition system (see Park paragraphs 0018-0019 and 0023).

With respect to claim 9, the data acquisition system, in response to receiving the control signal, overlays a recognizable pattern onto the video data such that the recognizable pattern appears on a viewing display when the video data is replayed (see Park paragraph 0069-0073).

With respect to claim 10, the recognizable pattern includes a text string that appears on the display when the video data is replayed at a later time (see Park paragraph 0069-0073).

With respect to claim 11, the text string is a clock value (see Park paragraph 0069-0073).

Claims 14-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Jones et al (U.S. Patent # 7,120,252). Jones with respect to claim 14, teaches an apparatus for maintaining video data, the apparatus comprising: a video data processor that receives video data from a video data acquisition system, the video data being stored in a first memory storage device (see Jones column 9 line 40 – column 11 line 35); and a hashing processor that generates a hash value based on a selected portion of the video data, the hash value being stored in the first memory storage device and a second memory storage device (see Jones column 9 line 40 – column 11 line 35).

With respect to claim 15, the selected portion of video data retrieved from the first memory storage device is authenticated by checking that the selected portion of video data from the first memory storage device, when hashed, produces a same hash value as the corresponding hash value stored in the second memory storage device (see Jones column 9 line 40 – column 11 line 35).

Claims 16, 21-25, 31 and 37-38 are rejected under 35 U.S.C. 102(e) as being anticipated by Peters (U.S. Patent Application Publication # 2003/0226023). With respect to claim 16, Peters teaches a method for generating an output signal from a video data acquisition system, the method comprising: receiving a video signal that varies depending on sensed images (see Peters paragraph 0004); encrypting the video signal using a first key; encrypting the first key using a second key; and including at least the encrypted first key and encrypted video signal in the output signal (see Peters paragraph 0031-0036).

With respect to claim 21, a method for maintaining video data, the method comprising: providing an encryption key to a video data acquisition system (see paragraph 0029); encrypting at least a portion of an output signal generated by the video data acquisition system using the provided encryption key (see Peters paragraph 0031-0036); and maintaining confidentiality of the provided encryption key so that recorded subjects of the video data acquisition system do not have access to the provided encryption key (see Peters paragraph 0033), knowledge of the provided encryption key being entrusted to an escrow agent (see Peters paragraph 0043).

With respect to claim 22, verifying an authenticity of the output signal by checking that at least a portion of the output signal is encrypted with the provided key (see Peters figure 1 and paragraph 0031-0036).

With respect to claim 23, notifying the escrow agent to decrypt selected portions of the output signal previously stored in memory using the provided encryption key (see Peters paragraphs 0040-0043).

With respect to claim 24, encrypting video data according to a hierarchical set of keys including the provided encryption key, at least one key of the hierarchical set of keys being used to encrypt another key associated with the output signal (see Peters paragraph 0031-0036).

With respect to claim 25, using the provided encryption key to encrypt at least one other encryption key associated with the output signal (see Peters paragraph 0031-0036).

With respect to 31, an apparatus to support surveillance, the apparatus comprising: a camera to generate a video signal that varies depending on sensed images; a memory device to store at least first and second encryption keys; and a processor that encrypts the video signal using the first encryption key, the processor encrypting the first encryption key with the second encryption key, the processor producing an output signal including at least the encrypted video signal and the encrypted first encryption key (see Peters paragraph 0004 and 0031-0036).

With respect to claim 37, an apparatus to support surveillance, the apparatus comprising: a camera to generate a video signal that varies depending on sensed images; a memory device to store at least first and second encryption keys; and means for encrypting the video signal using the first encryption key and means for encrypting the first encryption key with the second encryption key to produce an output signal including at least the encrypted video signal and the encrypted first encryption key (see Peters paragraph 0004 and 0031-0036).

With respect to claim 38, a computer program product including a computer-readable medium having instructions stored thereon for processing data information, such that the instructions, when carried out by a processing device, cause the processing device to perform the steps of: receiving a video signal that varies depending on sensed images; encrypting the video signal using a first key; encrypting the first key using a second key, the first and second key being different than each other; and including at least the encrypted first key and encrypted video signal in the output signal (see Peters paragraph 0004 0031-0036).

Claims 26, 28-30 and 36 are rejected under 35 U.S.C. 102(b) as being anticipated by Chainer et al (U.S. Patent # 6,397,334). Chainer with respect to claim 14, teaches With respect to claim 26, a method for generating an output signal from a video data acquisition system, the method comprising: receiving a video signal that varies depending on images detected by a video camera; encrypting a selected portion of the video signal using a first encryption key (see Chainer figure 2 and 3, column 4 line 30 –

column 6 line 17 and column 7 lines 52-61); receiving a sensor signal that varies depending on detection of objects in a vicinity of the data acquisition system (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61); and encrypting a selected portion of the sensor signal using a second encryption key (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61); and producing the output signal to include at least the encrypted video signal and the encrypted sensor signal (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61).

With respect to claim 28, generating the output signal to include multiple tracks, one of the tracks including the encrypted video signal arid the encrypted first key, another track including sensor data provided by a sensor associated with the video data acquisition system (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61).

With respect to claim 29, generating the other track includes generating encrypted RFID (Radio Frequency Identification) information (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61).

With respect to claim 30, implementing a recognition algorithm to identify objects associated with the sensed images; and in response to recognition of an object associated with the sensed images, embedding encrypted data information identifying the recognized object in the output signal (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61).

With respect to claim 36, an apparatus to support surveillance, the apparatus comprising: a video camera that generates a video signal that varies depending on sensed images; a sensor device that generates a sensor signal depending on detection of objects in a vicinity of the video camera; and a processor in communication with the memory device that encrypts the video signal using a first key and encrypts the sensor signal using a second key, the processor producing an output signal to include at least the encrypted video signal and encrypted sensor signal (see Chainer figure 2 and 3 and column 4 line 30 – column 6 line 17)..

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Park (U.S. Patent Application Publication # 2004/0085445) in view of Peters (U.S. Patent Application Publication # 2003/0226023). Park teaches everything with respect to claim 1, above but with respect to claim 3, does not teach maintaining confidentiality of the key so that recorded subjects of the video data acquisition system do not have access to the key; and entrusting an escrow agent with knowledge of the key. Peters teaches maintaining confidentiality of the key so that recorded subjects of the video data acquisition system do not have access to the key (see Peters paragraph 0033); and entrusting an escrow agent with knowledge of the key (see Peters paragraph 0043). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have maintained confidentiality of the keys so that the keys could not get into the wrong hands. One would be motivated to maintained confidentiality of the keys to make sure that the video has a strong encryption and cant be tampered with.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Park (U.S. Patent Application Publication # 2004/0085445) in view of Jones et al (U.S. Patent # 7,120,252). Park teaches everything with respect to claim 1 above but with respect to claim 6 Park does not teaches providing a control signal that identifies a hashing function to be used for hashing at least a portion of the video data; and at least occasionally receiving hashed values associated with portions of the video data in lieu of receiving a substantially continuous stream of corresponding non-hashed video data. Jones teaches providing a control signal that identifies a hashing function to be used for hashing at least a portion of the video data; and at least occasionally receiving hashed values associated with portions of the video data in lieu of receiving a substantially continuous stream of corresponding non-hashed video data (see Jones column 9 line 40 – column 11 line 35). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have hashed the video with a hash function before transmitting the encrypted raw video and the hash value over a network. Then hashing the raw video again on the receiving device and checking to see if the hash values are equal as a way to make sure that the video has not been tampered with. One would be motivated to do this to make sure that the video has not been tampered with.

Claim 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones et al (U.S. Patent # 7,120,252) in view of Greene (U.S. Patent # 6870929). Jones teaches with respect to claim 12, a method for maintaining video data, the method comprising: receiving video data from a video data acquisition system (see abstract and column lines 3-57); hashing a selected portion of the video data to produce a hash value (see Jones column 9 line 40 – column 11 line 35); storing the selected portion of the video data and corresponding hash value in a first memory storage device; and transmitting the corresponding hash value for storage in a second memory storage device (see Jones column 9 line 40 – column 11 line 35). Jones does not teach that the transmitting of video is over a network. Greene teaches that the transmitting of encrypted video is over a network (see column 1 lines 30-59). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have transmitting the encrypted video a network where it is imposable to have a direct connection between the video camera and the display device. One would be motivated to have sent video over a network to watch the video at a location where it is to far to make a direct connection between the video camera and the display device.

With respect to claim 13, retrieving the selected portion of video data from the first memory storage device; and verifying an authenticity of the selected portion of the video data by checking that the selected portion of video data, when hashed, produces a same hash value as the corresponding hash value stored in the second memory storage device (see Jones column 9 line 40 – column 11 line 35).

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peters (U.S. Patent Application Publication # 2003/0226023) in view of Schier (U.S. Patent # 6,907,123). Peters teaches everything with respect to claim 16 above but with respect to claim 17 it does not teach randomly generating a new encryption key for encrypting different portions of the video signal over time. Schier teaches randomly generating a new encryption key for encrypting different portions of the video signal over time (see Schier column 3 line 11 – column 4 line 29 and column 8 lines 26-36). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to generating a new encryption key for encrypting different portions of the video signal over time to increase the security of the transfer by changing the encryption thought out the transfer. One would be motivated to have randomly generating a new encryption key for encrypting different portions of the video signal over time to further increase seccurity.

Claim 18-20 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peters (U.S. Patent Application Publication # 2003/0226023) in view of Chainer et al. (U.S. Patent # 6,397,334). Peters teaches everything with respect to claim 16 and 31 above but with respect to claim 18 and 33, does not teach generating the output signal to include multiple tracks, one of the tracks including the encrypted video signal and the encrypted first key, another track including sensor data provided by a sensor associated with the video data acquisition system, the sensor data also being encrypted using an encryption key. Chainer teaches generating the output signal to include multiple tracks, one of the tracks including the encrypted video signal and the encrypted first key, another track including sensor data provided by a sensor associated with the video data acquisition system, the sensor data also being encrypted using an encryption key (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have encrypted the video and sensor (RFID) data before transmitting it over a network the help the receiver authenticate the image since each object has a unique RFID assigned to it the receiver knows if what they are told they are looking is really what they are looking at. One would be motivated to have encrypted the video and sensor (RFID) data before transmitting it over a network the help the receiver authenticate the image since.

With respect to claim 19 and 34, Peters teaches everything with respect to claim 16 and 31 above but with respect to claim 19 and 34 does not teach generating the other track includes generating encrypted RFID (Radio Frequency Identification) information. Chainer teaches generating the other track includes generating encrypted RFID (Radio Frequency Identification) information (see Chainer figure 2 and 3, column

4 line 30 – column 6 line 17 and column 7 lines 52-61). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have included an unique RFID number assigned to it to help the receiver knows if what they are told they are looking is really what they are looking at. One would be motivated to have included an (RFID) data before transmitting it over a network the help the receiver authenticate the object in the image since.

With respect to claim 20 and 35, Peters teaches everything with respect to claim 16 and 31 above but with respect to claim 20 and 35 does not teach implementing a recognition algorithm to identify objects associated with the sensed images; and in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal. Chainer teaches implementing a recognition algorithm to identify objects associated with the sensed images; and in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have recognized object based on RFID tags, iris/retinal shape, dental configuration and other characteristic and transmit then in encrypted from to help the receiver authenticate what he is looking at. One would be motivated to have sent sensor data encrypted to help the receiver authenticate what he is looking at.

Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chainer et al (U.S. Patent # 6,397,334) in view of Schier (U.S. Patent # 6,907,123). Chainer teaches everything with respect to claim 26 above but with respect to claim 27 Chainer does not teach randomly generating a new encryption key for encrypting different portions of the video signal over time. Schier teaches randomly generating a new encryption key for encrypting different portions of the video signal over time (see Schier column 3 line 11 – column 4 line 29 and column 8 lines 26-36). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to generating a new encryption key for encrypting different portions of the video signal over time to increase the security of the transfer by changing the encryption thought out the transfer. One would be motivated to have randomly generating a new encryption key for encrypting different portions of the video signal over time to further increase security.

Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peters (U.S. Patent Application Publication # 2003/0226023) in view of Schier (U.S. Patent # 6,907,123). Peters teaches everything with respect to claim 31 above but with respect to claim 32 Peters does not teach randomly generates a new value for the first encryption key to uniquely encrypt different portions of the video signal over time. Schier teaches randomly generates a new value for the first encryption key to uniquely encrypt different portions of the video signal over time (see Schier column 3 line 11 – column 4 line 29 and column 8 lines 26-36). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to generating a new encryption key for encrypting different portions of the video signal over time to increase the security of the transfer by changing the encryption thought out the transfer. One would be motivated to have randomly generating a new encryption key for encrypting different portions of the video signal over time to further increase security.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA

Devin Almeida
Patent Examiner
10/19/2006

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100